Carnegie Mellon University
Tepper School of Business

William Larimer Mellon, Founder

Dr. Ariel Zetlin-Jones, Associate Professor of Economics, Tepper School of Business, Carnegie Mellon University

Ariel Zetlin-Jones is an Associate Professor of Economics at the Tepper School of Business, Carnegie Mellon University. He received his Ph.D. in Economics from the University of Minnesota in 2012 and his Bachelor of Arts from Williams College in 2004. His research focuses on developing a better understanding of the workings of financial markets with implications for the design of optimal financial regulations. Since 2016, Ariel has been researching the economics of blockchains: how economic incentives may be used to shape blockchain consensus and stable coin protocols as well as the novel and economically large centralized markets that currently support cryptocurrency trading. His research has been published in the American Economic Review, the Journal of Political Economy, and the Journal of Monetary Economics. Ariel is also a Co-Director of Carnegie Mellon's Secure Blockchain Initiative and a Co-Principal Investigator for the Algorand Centre of Excellence at Carnegie Mellon.

The Secure Blockchain Initiative @ CMU

Presentation to Pennsylvania House State Government Committee

Ariel Zetlin-Jones

August 24, 2022

Blockchain@CMU

- Faculty Co-Directors:
  - **Nicolas Christin** (Engineering and Public Policy, Institute for Software Research)
  - **Elaine Shi** (Computer Science, Electrical and Computer Engineering)
  - **Ariel Zetlin-Jones** (Tepper School of Business)
- Cross-College, Cross-Campus, Cross-Continent Collaboratory
  - Existing Partners: Ripple, Algorand Foundation, Crypto.Com
- Funding deep, technical research for blockchain and blockchain applications
- Developing blockchain curriculum for students and the wider public (picoCTF)

Our Research and Curriculum

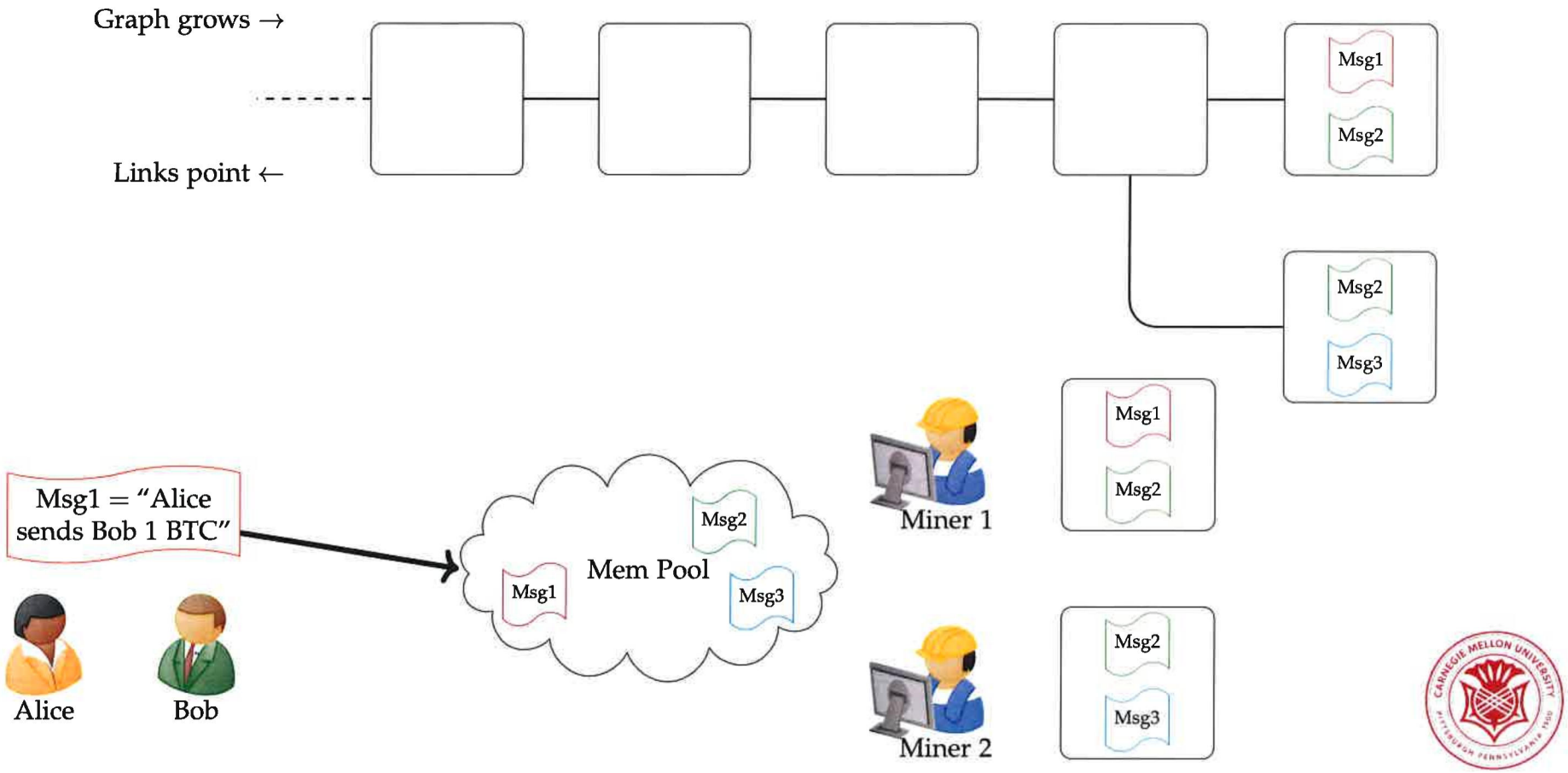
- Blockchain Scalability
- Economics, Incentives, and Security
- Cryptography and Privacy
- Programming for Blockchains
- Markets, Policy, and Regulation

What is Blockchain and Why is it Secure?

Blockchain

- New way to generate "shared memory"
- Formally, blockchain is a decentralized, distributed ledger
- One application of shared memory $\Rightarrow$ Money
- Shared memory without trust requires incentives $\Rightarrow$ Cryptocurrency

Blockchain: An Illustration



Human Behavior Secures Blockchain Data

- Blockchain powered by:
  - Distributed Systems
  - Cryptography
  - Incentives
- Blockchain at the intersection of human behavior and technology
- Incentives and behavior a key component of blockchain security
  - Are miners validating the "correct" transactions
  - Incentives to validate correctly needed to ensure "immutability" of the blockchain

What is Blockchain's Potential?

What Can we Do with Immutable Ledgers?

- We can store "balances" on the blockchain
- In principle, can store *any* data on the blockchain
  - Computer software at its core is "just" data
  - Blockchains like Ethereum permit you to store software on its blockchain
  - We call this software "smart contracts"
- Once we store software on the blockchain, we may ask miners to execute and record outcome of software to the blockchain
  - ☞ Distributed "cloud computer"

Programmable Money and Security

- Most current applications: monetary and financial applications
- Build smart contracts to permit programmable transfers
- Smart Contract Examples (*Decentralized Finance*)
  - Automated Market Makers
  - Collateralized Lending
  - Stablecoins
    ☞ See Routledge and Zetlin-Jones (2022), `https://doi.org/10.1016/j.jedc.2021.104155`
- Smart contracts introduce new sources of risk
  - Security risk from implementation/code complexity
  - Security risk from faulty business models

DeFi Attacks (60+ Billion USD, 2000+ Incidents)

- Wallet & client-side Operational Security
  - Solana Slope seed-phrase leak
  - Phishing of Uni V3 LP tokens
- Bridge Hacks (Contract code & Developer Operational Security)
  - Wormhole
  - Nomad
  - Axie Infinity
  - Harmony One
  - Ronin
- Incentive design failure/faulty business model
  - LUNA+UST
  - Iron Finance, Empty Set, Basis Cash, SafeCoin, BitUSD, DigitalDollar, NuBits, and CK USD
- Poor assumptions / Oracle Attack
  - KAVA assumed UST = $1, worthless collateral used to borrow valuable assets
  - Swift market movements & high block demand lead to sever oracle lag
  - Aave vault held by 0x4093fbe60ab50ab79a5bd32fa2adec255372f80e failed to be liquidated twice due to Chainlink oracle lag

Blockchain's Potential

- Shared memory/record keeping is hard and valuable
  - Even "trusted" party systems rely on complex incentives via reputation and regulation
- Blockchain proposes new approach to shared memory
- Blockchain disrupting economic systems where many individuals or businesses share information
  - Supply chains, health care records, sustainability, financial intermediation
- Blockchain smart contracts and systems are very complex
  - Complexity typically favors highly sophisticated players
  - Regulatory/Investor protections, long-term research, and sandboxes likely support useful innovation in the future